

PATENT ABSTRACTS OF JAPAN

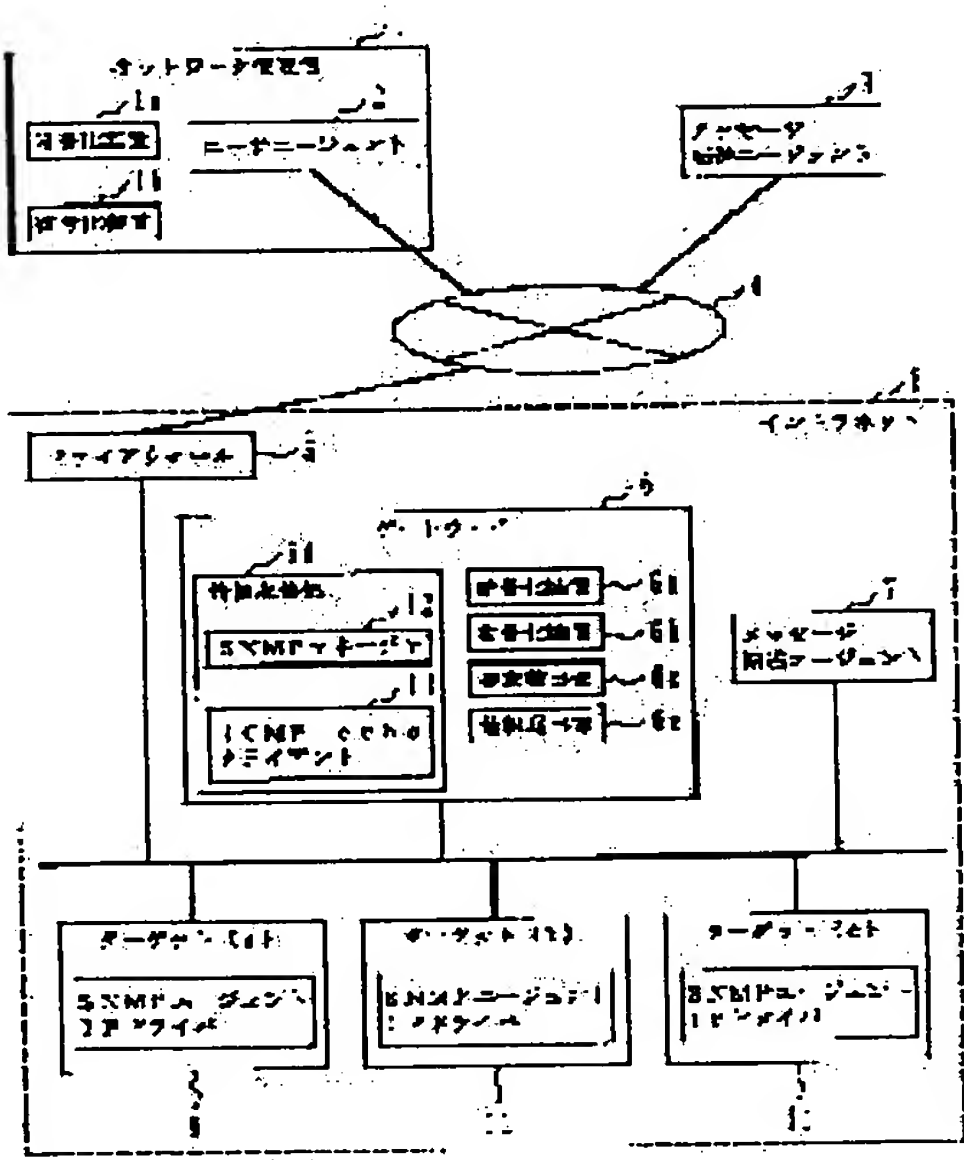
(11)Publication number : 11-150532
(43)Date of publication of application : 02.06.1999

(51)Int.Cl. H04L 12/24
H04L 12/26
G06F 13/00
G06F 13/00
H04L 12/66

(21)Application number : 09-316740 (71)Applicant : HITACHI INFORMATION SYSTEMS LTD
(22)Date of filing : 18.11.1997 (72)Inventor : ABE SHUNSUKE

(54) REMOTE MANAGEMENT SYSTEM FOR INTRA-NET AND STORAGE MEDIUM STORING PROGRAM USED FOR IT

(57)Abstract
PROBLEM TO BE SOLVED: To provide the remote management system for an intra-net which enables remote management of the intra-net via the internet so as to reduce a network management cost and to provide the storage medium that records a program used for the system.
SOLUTION: A gateway 6 is provided with a request detection section 6c that reads an intra-net management information request from a message in electronic mail sent to the intra-net 8 via the Internet 4, an information collection section 6d that collects the intra-net management information corresponding to the intra-net management information request read, and an information transmission section 6e that returns the collected intra-net management information as a message in electronic mail via the internet 4. The intra-net 8 having a firewall 5 is managed by using the electronic mail via the internet 4.



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-150532

(43)公開日 平成11年(1999) 6 月 2 日

(51)Int.Cl.⁵
H 0 4 L 12/24
12/26
G 0 6 F 13/00
H 0 4 L 12/66

識別記号
3 5 1
3 5 3

F I
H 0 4 L 11/08
G 0 6 F 13/00
H 0 4 L 11/20
3 5 1 G
3 5 3 U
B

審査請求 未請求 請求項の数4 O L (全 9 頁)

(21)出願番号 特願平9-316740

(22)出願日 平成9年(1997)11月18日

(71)出願人 000152985

株式会社日立情報システムズ
東京都渋谷区道玄坂1丁目16番5号

(72)発明者 安部 俊輔

東京都渋谷区道玄坂一丁目16番5号 株式
会社日立情報システムズ内

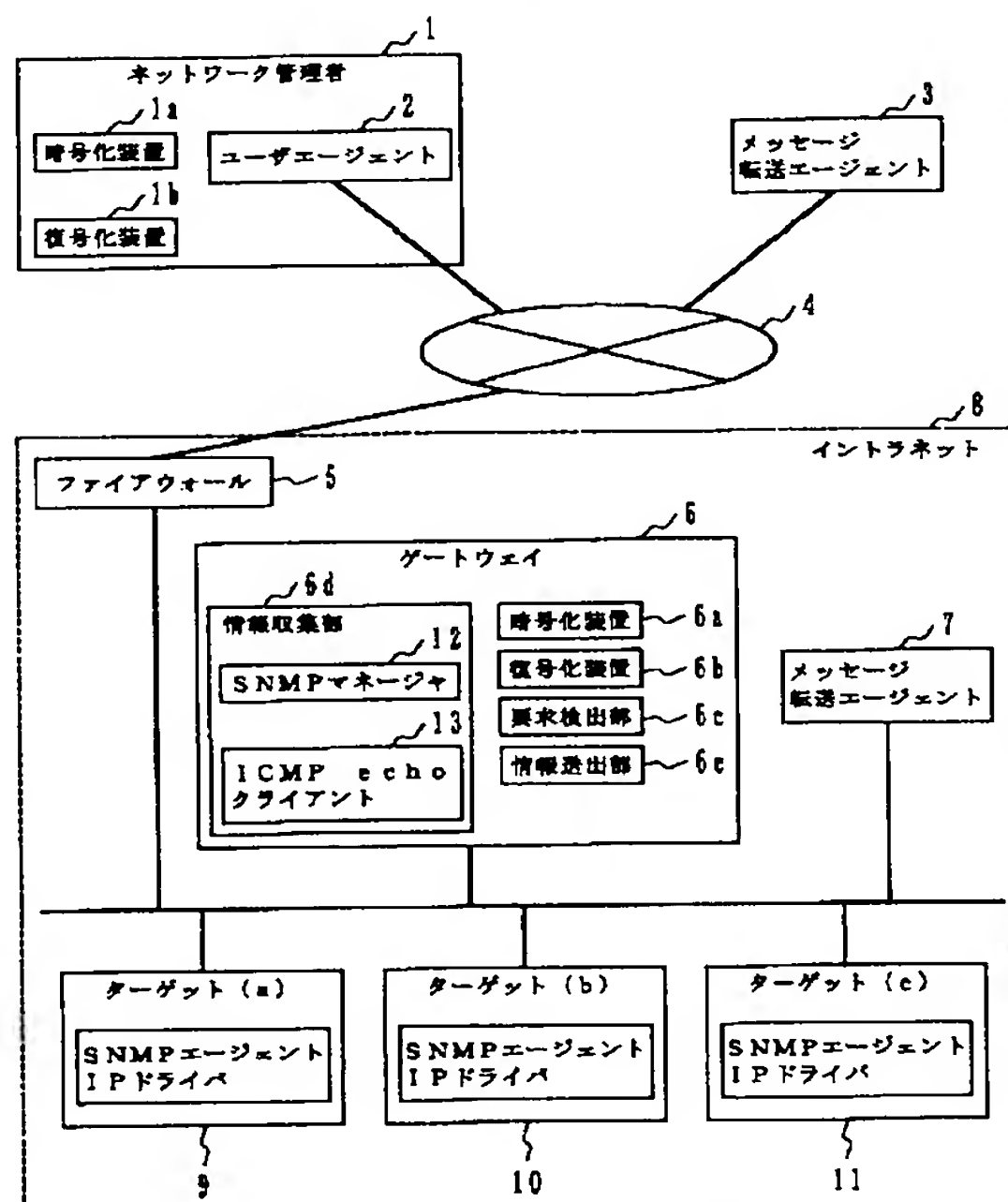
(74)代理人 弁理士 磯村 雅俊 (外1名)

(54)【発明の名称】 イントラネットの遠隔管理システムおよびこれに用いるプログラムを記録した記録媒体

(57)【要約】

【課題】 インターネット経由で、ファイアウォールが設けられたイントラネットの遠隔管理ができない。

【解決手段】 インターネット4経由でイントラネット8に送られてきた電子メール中のメッセージからイントラネットの管理情報要求を読み取る要求検出部6cと、読み取ったイントラネットの管理情報要求に対応してイントラネットの管理情報を収集する情報収集部6dと、収集したイントラネットの管理情報を電子メール中のメッセージとしてインターネット4経由で返送する情報送出部6eとをゲートウェイ6に設け、ファイアウォール5を有するイントラネット8の管理をインターネット4経由で電子メールを用いて行う構成とする。



【特許請求の範囲】

【請求項 1】 ファイアウォールを介してインターネットと接続されたイントラネットの管理を行うシステムであって、上記インターネット経由で上記イントラネットに送られてきた電子メールを受信し、該電子メール中のメッセージから上記イントラネットの管理情報要求を読み取る第 1 の手段と、該第 1 の手段で読み取った上記イントラネットの管理情報要求に対応してイントラネットの管理情報を収集する第 2 の手段と、該第 2 の手段で収集したイントラネットの管理情報を電子メール中のメッセージとして上記インターネット経由で返送する第 3 の手段とを有し、上記ファイアウォールを介して接続されたイントラネットの管理をインターネット経由で電子メールを用いて行うことを特徴とするイントラネットの遠隔管理システム。

【請求項 2】 請求項 1 に記載のイントラネットの遠隔管理システムにおいて、上記第 1 の手段で読み取る上記電子メール中のメッセージから予め暗号化された上記イントラネットの管理情報要求を復号化する復号化手段と、上記第 3 の手段で上記電子メール中のメッセージとして返送する上記イントラネットの管理情報を暗号化する暗号化手段とを設け、上記イントラネットの管理情報を暗号化して上記インターネット上に送出することを特徴とするイントラネットの遠隔管理システム。

【請求項 3】 請求項 2 に記載のイントラネットの遠隔管理システムにおいて、上記第 1 の手段と上記第 2 の手段および上記第 3 の手段、ならびに、上記復号化手段と上記暗号化手段を、上記イントラネット上のゲートウェイに設けたことを特徴とするイントラネットの遠隔管理システム。

【請求項 4】 ファイアウォールを介してインターネットと接続されたイントラネットの遠隔管理を行うコンピュータで用いるプログラムを記録した記録媒体であって、上記イントラネットの遠隔管理を行うコンピュータに、上記インターネット経由で上記イントラネットに送られてきた電子メールを受信し、該電子メール中のメッセージから上記イントラネットの管理情報要求を読み取る第 1 の手順と、該第 1 の手順で読み取った上記イントラネットの管理情報要求に対応してイントラネットの管理情報を収集する第 2 の手順と、該第 2 の手順で収集したイントラネットの管理情報を電子メール中のメッセージとして上記インターネット経由で返送する第 3 の手順とを含み、上記ファイアウォールを介して接続されたイントラネットの遠隔管理をインターネット経由で電子メールを用いて行わせるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、コンピュータネットワークの遠隔管理技術に係わり、特に、イントラネッ

トの遠隔管理を効率的に行うのに好適なイントラネットの遠隔管理システムおよびこれに用いるプログラムを記録した記録媒体に関するものである。

【0002】

【従来の技術】 近年のインターネットの普及により、国や組織の境界を越えてコンピュータ同士の通信が可能になっている。また、イントラネットと呼ばれるインターネットの技術を取り入れて企業内のコンピュータネットワークを構築するケースが増えている。

10 【0003】 このイントラネットでは TCP/IP (Transmission Control Protocol/Internet Protocol) をベースとした通信が行われ、例えば、「97年版 情報・通信新語辞典」(1977年、日経BP社発行)の第529～530頁に記載のように、SNMP (Simple Network Management Protocol) によるネットワーク管理が行なわれる。

20 【0004】 従来、遠隔地からイントラネットの管理を行う場合には、専用線やダイヤルアップ回線を設置することが行われていた。しかし、専用線は、一定の帯域が保証される一方で、一般的に通信費が高い。また、ダイヤルアップ回線は、通常の加入電話回線でモデム同士を接続するものであり、設備は廉価であるが、遠距離市外通話では通信費が割高になるという問題点があった。インターネットを利用すれば、ダイヤルアップ回線であってもインターネットサービス提供者のアクセスポイントへの市内通話料のみを負担するだけで良いので通信費の削減に役立つ。

30 【0005】 しかし、インターネットに接続した各企業では、通常、セキュリティを確保するために、いわゆるファイアウォール(内部のローカルネットワークと外部のインターネットとの間に、外部からの不正なアクセスを防ぐ目的で設置されるコンピュータ)を用いてインターネットからのイントラネットへのパケットの流入を制限している。従って、インターネットからイントラネットの遠隔管理を行おうとしても、ファイアウォールが障害となってイントラネットへのアクセスができない。

【0006】

40 【発明が解決しようとする課題】 解決しようとする問題点は、従来の技術では、ファイアウォールが障害となってインターネットからイントラネットの遠隔管理アクセスができない点である。本発明の目的は、これら従来技術の課題を解決し、インターネット経由でのイントラネットの遠隔管理を可能とし、ネットワーク管理コストの削減を図ることができるイントラネットの遠隔管理システムおよびこれに用いるプログラムを記録した記録媒体を提供することである。

【0007】

50 【課題を解決するための手段】 上記目的を達成するため、本発明のイントラネットの遠隔管理システムは、イントラネット中に例えばゲートウェイ(二つのプロトコ

ルを相互に変換するコンピュータ)を設置し、このゲートウェイで、電子メールプロトコル(SMTP: Simple Mail Transfer Protocol)とネットワーク管理プロトコル(SNMP: Simple Network Management Protocol、および、ping: ICMP echo Protocol)とを相互に変換させる構成とする。すなわち、電子メールはファイアウォールを通過することができるので、ネットワーク管理者は、ネットワークの管理情報の取得・設定要求を電子メールの本文中に命令文として記述し、電子メールプロトコル(SMTP)を利用して、イントラネットに送信する。ゲートウェイは電子メールで要求を受信すると、イントラネット上の、管理対象のコンピュータに関する情報を取得あるいは設定し、その実行結果を電子メールの形で、ネットワーク管理者側に返信する。尚、電子メール中のメッセージはインターネット上を通過する際は暗号化することにより、インターネット上の第三者が参照できないようにする。

【0008】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。図1は、本発明のイントラネットの遠隔管理システムの構成の一実施例を示すブロック図である。本図1において、1はネットワーク管理者用のコンピュータ(図中、「ネットワーク管理者」と記載)、2はネットワーク管理者用のコンピュータ1が有するユーザエージェント(ユーザの代わりに電子メールのメッセージを送信・受信するプロセス)、3はネットワーク管理者用のコンピュータ1が利用するメッセージ転送エージェント(電子メールのメッセージを格納あるいは転送するプロセス)、4はインターネット、5はファイアウォール、6はゲートウェイ、7はイントラネット内のメッセージ転送エージェント、8はイントラネット、9~11はイントラネット8上の管理対象コンピュータ(図中、「ターゲット(a)~(c)」と記載)である。

【0009】メッセージ転送エージェント3は、インターネット4のサービス提供者が管理するコンピュータ上に存在する。ネットワーク管理者用のコンピュータ1とゲートウェイ6は、それぞれ、暗号化装置1a、6aと復号化装置1b、6bを有し、電子メールの内容の暗号化・復号化と、暗号・復号キーの生成を行う。

【0010】尚、第三者が傍受したメッセージを再送信することによる攻撃に対する防御のため、暗号化・復号化キーは1回の通信毎に一方方向ハッシュ関数を適用して更新されるものとする。また、暗号化アルゴリズムは、対照型アルゴリズム(暗号化アルゴリズムにおいて暗号化キーワードを復号化キーワードから計算でき、その逆も可能なものをいう)、例えば、DES(Data Encryption Standard)方式を利用することとする。

【0011】ネットワーク管理者用のコンピュータ1には、予め、光ディスク等の記録媒体を介して、イントラ

ネットの管理情報要求を本文にした電子メールを生成するプログラムが搭載されている。そして、ネットワーク管理者が、ネットワーク管理者用のコンピュータ1から電子メールにより、管理対象コンピュータ9~11の管理情報を要求する場合、電子メール中のメッセージは暗号化装置1aにより暗号化されてインターネット4上に送出され、ファイアウォール5を通過してイントラネット8に到達する。イントラネット8に到達した電子メールは、ゲートウェイ6の復号化装置6bにより、そのメッセージが復号化される。

【0012】また、ゲートウェイ6には、予め、光ディスク等の記録媒体に記録されたプログラムをハードディスク上等に読み込んで構成された要求検出部6cと情報収集部6dおよび情報送出部6eが設けられており、ゲートウェイ6は、まず、要求検出部6cにより、復号化装置6bで復号化した電子メール中のメッセージからイントラネットの管理情報要求を読み出し、次に、情報収集部6dにより、要求検出部6cで読み出したイントラネットの管理情報要求に対応してイントラネットの管理情報を収集する。

【0013】すなわち、この情報収集部6dは、SNMPマネージャ12およびICMPエコークライアント(図中、「ICMPエコークライアント」と記載)13を有し、このSNMPマネージャ12およびICMPエコークライアント13により、ネットワーク管理者用のコンピュータ1に代わって、管理対象コンピュータ9~11のSNMPエージェントおよびIPドライバとの通信処理を行い、ネットワーク管理情報を収集する。

【0014】そして、ゲートウェイ6は、この情報収集部6dで収集して暗号化装置6bで暗号化したイントラネットの管理情報を、情報送出部6eにより、電子メール中のメッセージとしてインターネット4経由でネットワーク管理者用のコンピュータ1に返送する。ネットワーク管理者用のコンピュータ1は、ゲートウェイ6からの電子メールを受信し、復号化装置1bによりメッセージを復号化し、ネットワーク管理者に、イントラネットの管理情報を提供する。このようにして電子メールを利用することで、ファイアウォール5を介して接続されたイントラネット8の管理をインターネット4経由で行うことができる。

【0015】次に、図2を用いて、このような構成のイントラネットの遠隔管理システムによるネットワーク管理の実施手順を詳細に説明する。図2は、図1におけるイントラネットの遠隔管理システムの動作手順例を示す説明図である。

【0016】ネットワーク管理者は、ネットワーク管理者用のコンピュータ1により、管理対象のネットワークアドレスとそれに加えてMIB(Management Information Base: ネットワーク管理プロトコルでアクセスされるオブジェクトの集合)の名称とそれに対して実行する

10

20

30

40

50

要求（リクエスト）をASN. 1（Abstract Syntax Notation One: コンピュータの機種に依存しない抽象的なデータ構造の記述文法）形式の命令文として作成する。尚、本メッセージの一例を後述の図4で示す。

【0017】このメッセージを暗号化装置1aを経由してユーザエージェント2に渡す。ユーザエージェント2は、予め定義された転送先（メッセージ転送エージェント3）にメッセージを送信する。このメッセージ転送エージェント3は、ファイアウォール5経由でイントラネット8内のメッセージ転送エージェント7にメッセージを転送し、メッセージ転送エージェント7は、ゲートウェイ6にメッセージを転送する。

【0018】ゲートウェイ6は、復号化装置6bによりメッセージを復号化し、SNMPマネージャ12、または、ICMPエコークライアント13のいずれか一方を呼び出す。SNMPマネージャ12は、命令文をSNMP PDU（Protocol Data Unit: あるレイヤ内のプロトコルマシンの間で交換されるデータオブジェクト）に翻訳し、管理対象コンピュータ9～11のSNMPエージェントへ情報の取得・設定要求を送信する。

【0019】管理対象コンピュータ9～11のSNMPエージェントは、情報の取得要求に対しては要求された情報を、情報の設定要求に対しては処理結果を、SNMP PDUとして、ゲートウェイ6のSNMPマネージャ12に返信する。また、ゲートウェイ6のICMPエコークライアント13は、管理対象コンピュータ9～11に、ICMPエコーリクエストメッセージを送信する。管理対象コンピュータ9～11は、IPドライバにより、ICMPエコーリクエストメッセージを受信すると、ICMPエコーリプライメッセージを送信元に返す。

【0020】ゲートウェイ6は、管理対象コンピュータ9～11からSNMPマネージャ12またはICMPエコークライアント13に返されたSNMP PDUやICMPエコーリクエストメッセージに基づき返信メッセージを作成する。尚、この返信メッセージの一例を後述の図5で示す。さらに、ゲートウェイ6は、返信メッセージを暗号化装置6aにより暗号化し、メール転送プロトコルを利用して、メッセージ転送エージェント7、ファイアウォール5を介してネットワーク管理者のメッセージ転送エージェント3に送信する。

【0021】メッセージ転送エージェント3は、返信メッセージをユーザエージェント2に転送し、ユーザエージェント2は、返信メッセージをネットワーク管理者用のコンピュータ1に転送する。返信メッセージは、復号化装置1bにより復号化される。このようにしてネットワーク管理者は、応答メッセージを得ることができる。次に、ゲートウェイ6がメッセージを受信した後の処理を、図3を用いて詳細に説明する。

【0022】図3は、図1におけるゲートウェイのメッ

セージ受信後の処理例を示すフローチャートである。まず、メッセージのSUBJECTフィールド（図4における符号41）をチェックし（ステップ250）、ネットワーク管理要求（「MANAGEMENT_REQUEST」）であると判定した場合、メッセージを復号化し（ステップ2

6）、語彙解析（ステップ270）および構文解析（ステップ280）を行う。それぞれの処理で、受信したメッセージに誤りがない場合、次のステップを実行するが、誤りがあった場合はエラーメッセージを返送する。

【0023】次に、ゲートウェイは、メッセージの指定によりSNMPマネージャまたはICMPエコークライアントのどちらかを呼び出す（ステップ290）。SNMPマネージャは、命令文（図4における符号42、43）をSNMP PDUに翻訳し、管理対象のコンピュータのSNMPエージェントに、情報の取得・設定要求を送信する（ステップ310）。SNMPエージェントは、情報の取得要求（「GetRequest」）に対しては要求された情報（図5における符号52）を、また、情報の設定要求（「SetRequest」）に対しては処理結果（図5における符号53）を、SNMP PDUとして返信する。

【0024】また、ICMPエコークライアントは、管理対象のコンピュータにICMPエコーリクエストメッセージ（図4における符号44: 「ping 9.1.2.8」）を送信する（ステップ300）。管理対象のコンピュータのIPドライバは、ICMPエコーリクエストメッセージ（ping）を受信すると、ICMPエコーリプライメッセージ（図5における符号54: 「9.1.2.8 is alive」）を送信元に返す。ここで、もしターゲットのIPドライバが起動していない場合、あるいはネットワークの障害が発生した場合、ICMPエコーリプライメッセージは返らない。この場合、ICMPエコークライアントはタイムアウトエラーをゲートウェイに通知する。

【0025】さらに、ゲートウェイは、SNMPマネージャまたはICMPエコークライアントから返されたSNMP PDUやICMPエコーリプライメッセージを人間が読める情報に翻訳し（ステップ320）、後述の図5に示す返信メッセージを作成する。そして、作成した返信メッセージを、暗号化装置で暗号化し（ステップ330）、メール転送プロトコルを利用してネットワーク管理者のメッセージ転送エージェントに送信する（ステップ340）。

【0026】このようにして、ゲートウェイから送信された返信メッセージは、ユーザエージェント経由でメッセージ転送エージェントからネットワーク管理者のコンピュータに転送され、さらに、復号化装置により復号化され、ネットワーク管理者は、応答メッセージを得ることができる。

【0027】図4は、図1のネットワーク管理者用のコンピュータから送出された電子メールの具体例を示す説

明図である。本メッセージにおいて、41はヘッダ部を、42はSNMP Getリクエストを、43はSNMP Setリクエストを、44はICMPエコーリクエストを表す。ヘッダ部のSUBJECTフィールドの値には予め取り決めておいた「ネットワーク管理要求」を意味する文字列が設定されている。

【0028】図5は、図1のゲートウェイから送出された電子メールの具体例を示す説明図である。本例は、図1のゲートウェイから送出された返信メッセージであり、51はヘッダ部を、52～54はそれぞれ図4のSNMP Getリクエスト42、SNMP Setリクエスト43、ICMPエコーリクエスト44に対応する応答文である。この返信メッセージは、図1におけるゲートウェイ6の暗号化装置6aにより暗号化され、メール転送プロトコルでネットワーク管理者のメッセージ転送エージェントに送信される。

【0029】以上、図1～図5を用いて説明したように、本実施例のイントラネットの遠隔管理システムでは、ネットワーク管理者は、電子メールを利用し、イントラネット内に設置されたゲートウェイに命令文を送信して、イントラネット上のコンピュータの情報の問い合わせ・設定を行い、その実行結果を電子メールにて受け取る。このように、ファイアウォールを透過可能なプロトコルである電子メールを利用して、インターネット経由でイントラネットの遠隔管理を行なうことにより、ネットワーク管理コストの削減を図ることができる。

【0030】特に、既にインターネットに接続されている企業においては、セキュリティのレベルを維持しながら、専用回線の増設などの設備投資を行うことなしに、ゲートウェイの追加のみで、イントラネットの遠隔管理を行うことが可能となり、ネットワークの維持コストの低減を実現することが可能となる。

【0031】尚、本発明は、図1～図5を用いて説明した実施例に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能である。例えば、本例で

は、図1に示すように、ゲートウェイ6に暗号化装置6aや、復号化装置6b、要求検出部6c、情報収集部6d、および情報送出部6eの各処理部を設けた構成としたが、これらの各処理部をイントラネット8内に設ける構成であれば、この構成に限定されるものではない。

【0032】

【発明の効果】本発明によれば、インターネット経由で、ファイアウォールが設けられたイントラネットの遠隔管理が可能となり、ネットワーク管理コストの削減を図ることができる。

【図面の簡単な説明】

【図1】本発明のイントラネットの遠隔管理システムの構成の一実施例を示すブロック図である。

【図2】図1におけるイントラネットの遠隔管理システムの動作手順例を示す説明図である。

【図3】図1におけるゲートウェイのメッセージ受信後の処理例を示すフローチャートである。

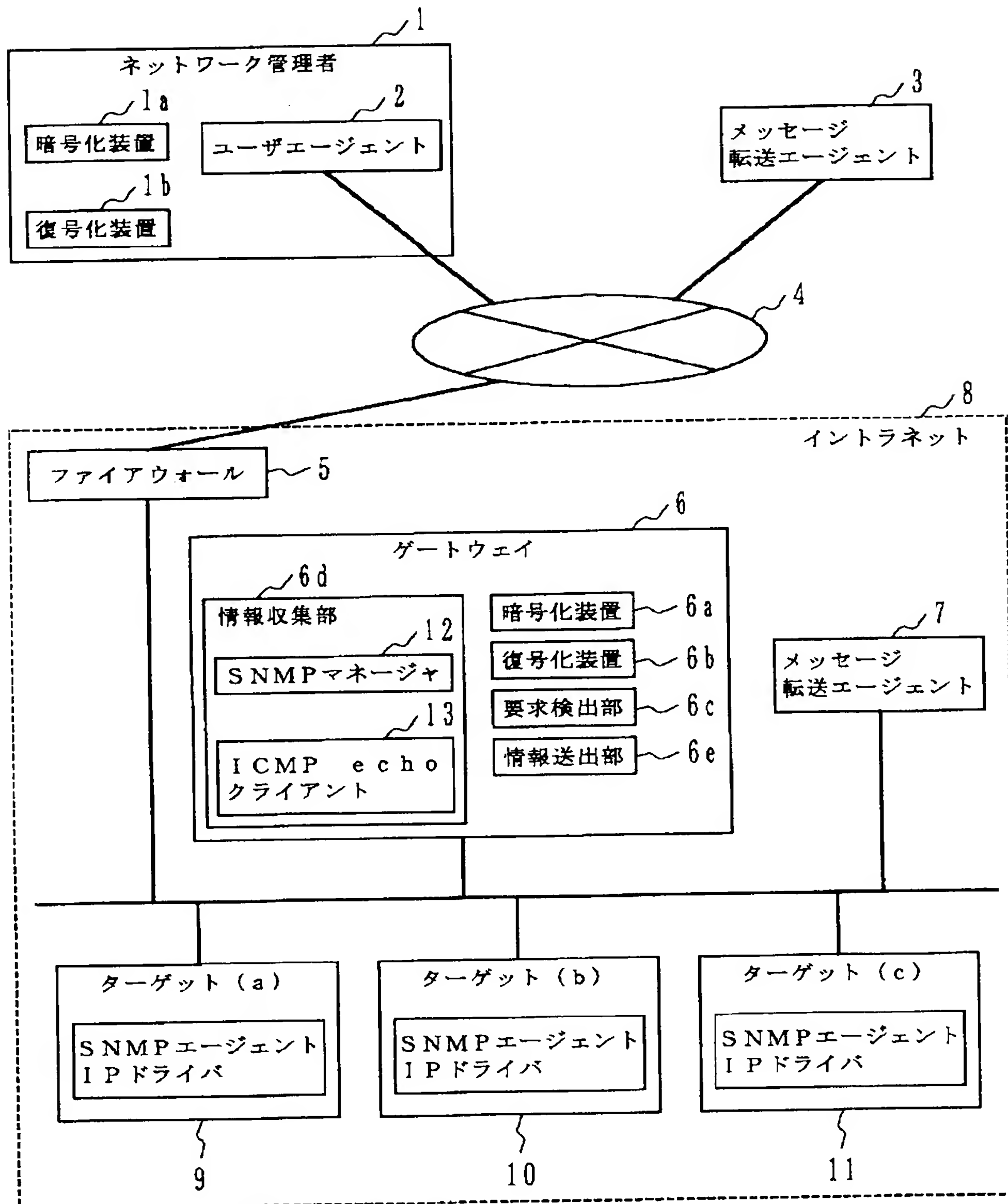
【図4】図1のネットワーク管理者用のコンピュータから送出された電子メールの具体例を示す説明図である。

【図5】図1のゲートウェイから送出された電子メールの具体例を示す説明図である。

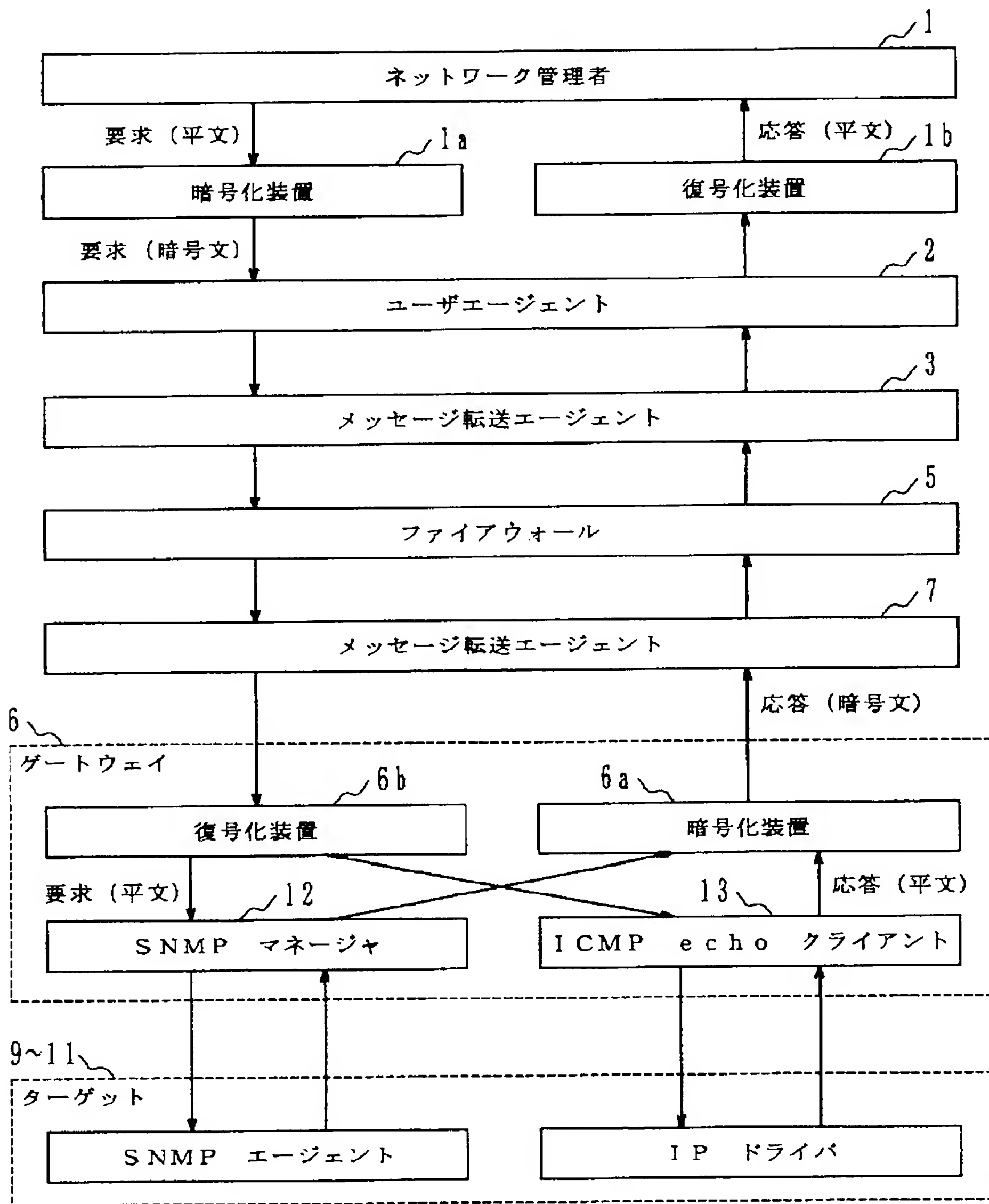
【符号の説明】

1：ネットワーク管理者用のコンピュータ、1a：暗号化装置、1b：復号化装置、2：ユーザエージェント、3：メッセージ転送エージェント、4：インターネット、5：ファイアウォール、6：ゲートウェイ、6a：暗号化装置、6b：復号化装置、6c：要求検出部、6d：情報収集部、6e：情報送出部、7：メッセージ転送エージェント、8：イントラネット、9～11：管理対象コンピュータ、12：SNMPマネージャ、13：ICMPエコークライアント、41：ヘッダ部、42：SNMP Getリクエスト、43：SNMP Setリクエスト、44：ICMPエコーリクエスト、51：ヘッダ部、52～54：応答文。

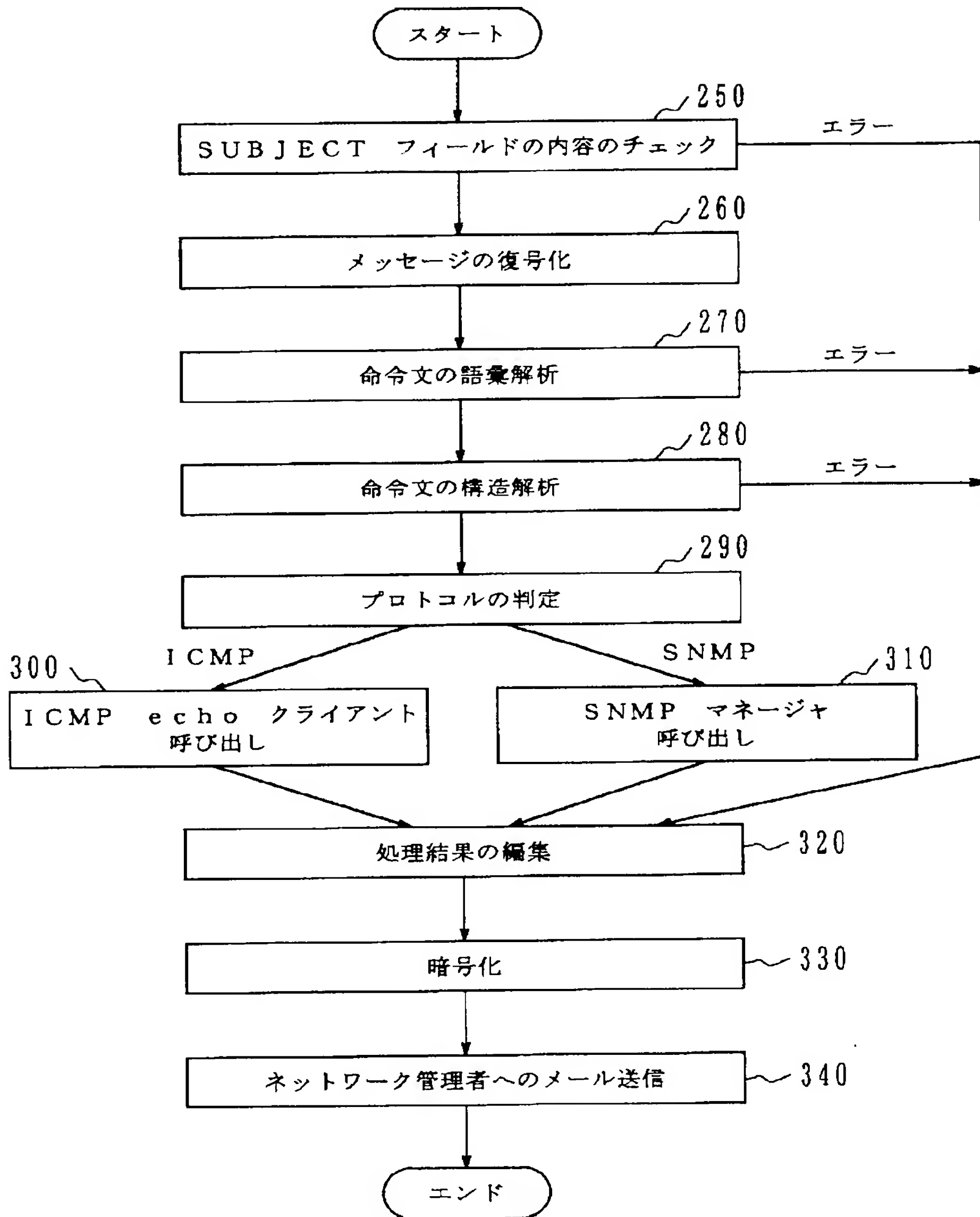
【図1】



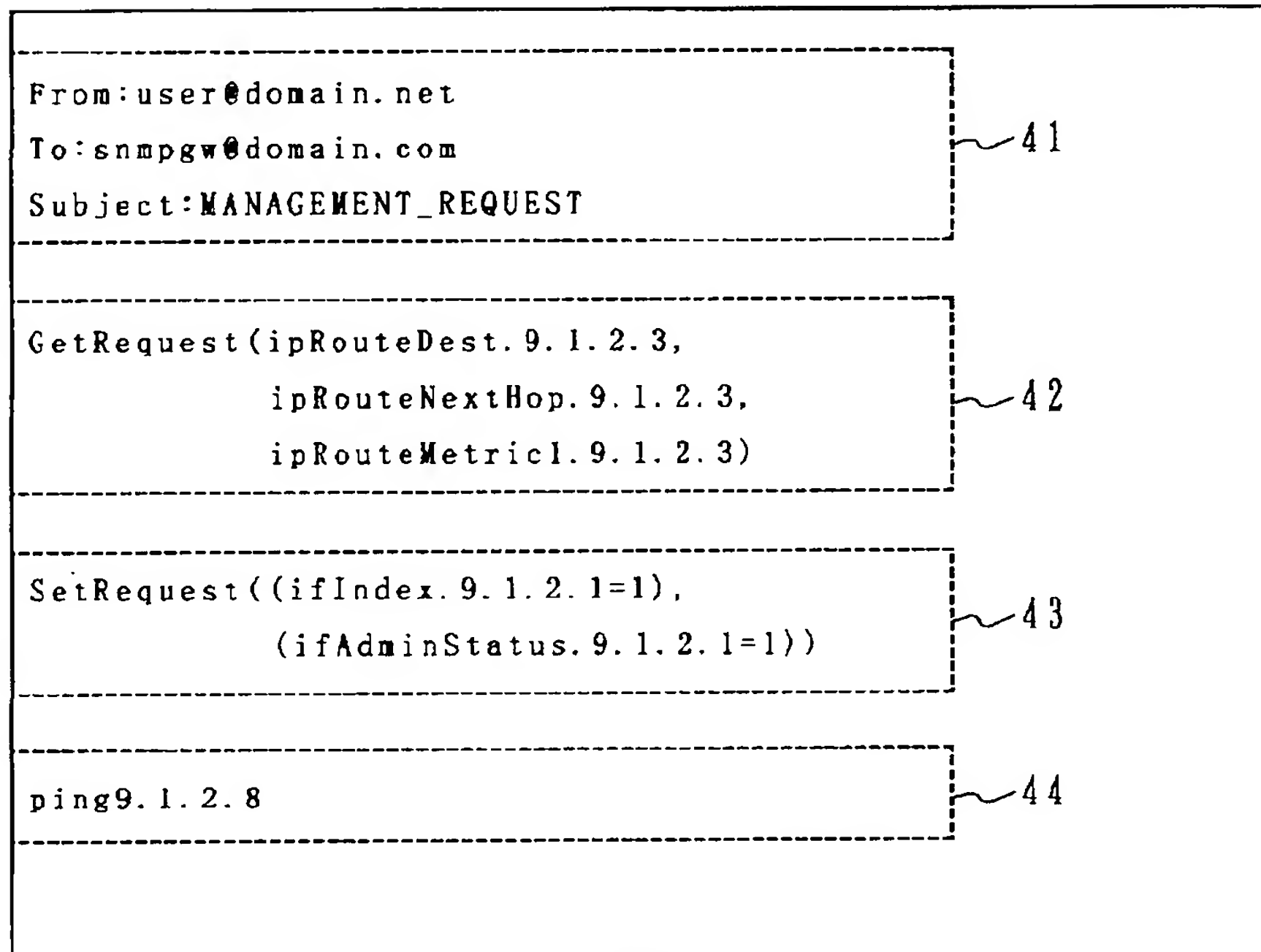
【図2】



【図3】



【図4】



【図5】

